

Piyasa işlemcilerinin güvenliği hakkında



ÇETİN KAYA
KOÇ

Bu ve bundan sonraki bir kaç yazıda dizüstü, masaüstü ve sunucu bilgisayarlar da kullanılan işlemciler yapılabilecek saldırılardan bahsedeceğiz.

Dizüstü, masaüstü ve sunucu bilgisayarlar da kullanılan işlemciler (Pentium, AMD, PowerPC, vb.) güvenlik mekanizmalarını işletir ve güvenlik fonksiyonlarını koştururken, gizli anahtarlar kullanılır. Örneğin elektronik imza icra eden bir işlemcinin, sunucunun RSA gizli anahtarına ulaşması ve onun yardımı ile RSA fonksiyonunu icra etmesi gerekir. Ancak piyasa işlemcileri gizli anahtarları elde etmek, tutmak ve saklamak, ve onlarla işlem yapmak için tasarlanmadığı için, standart kripto cihazlarında olduğu kadar güvenli işlem yapamayabilirler. Özellikle yazılım tasarlama bunun farkında değilse, işlemci bu anahtarlarla işlem yaparken, bazı kritik bilgiler kolaylıkla dışarıya sızabilir. Side-channel (yan-kanal) analizi diye adlandırdığımız metotlarla böyle işlemcileri izlemek ve gizli anahtarları elde etmek mümkündür. Bu ve bundan sonraki bir kaç yazıda, size bu konulardan bahsetmek istiyorum.

İşlemcilerde yapılan bu tip saldırılar, iki kategoride toplanabilir: Uzaktan (remote) saldırılar ve içeriden (intraprocessor) saldırılar. Uzaktan saldırılarda, saldırı şifrelemesi için sunucuya mesaj dizileri gönderir ve her bir mesajın şifrelenip geri gelmesi için harca-

nan zamanı ölçer. Tabii aradaki ağ sisteminin bu zaman üzerinde istatistiksel etkisi de göz önüne alınmalıdır. RSA algoritmasının her bir mesaj blokunu şifrelemek için harcadığı zamanın, RSA anahtarının bitlerinin değerlerine olan bağımlılığı yüzünden, bu ölçülen zamanlar analiz edilip, anahtarın tümünü veya bir kısmını öğrenmek mümkündür. Özellikle SSL sunuculara yapılan bu tip saldırılara "remote timing attacks" denir ve başarılı olabilecekleri kanıtlanmıştır.

İkinci tip saldırılarda, bizim sunucu üzerinde bir casus program oluşturmamız gerekir. Bu casus program, hafıza sistemin korunması yüzünden tabii ki başka bir programın verisini okuyamaz. Örneğin, şifreleme programı cache ünitesini kullanıyorsa, casus programının kendi zamanı yavaşladığından, bunu farkedebilir. Böyle bir üniteyi kullanma nedeni veya biçimi ile gizli anahtar bitlerinin değerleri arasında da bir ilişki olduğundan, gizli anahtarın tümünü veya bir kısmını öğrenebiliriz. Doktora öğrencim Onur Acıçmez ile birlikte bu konuda yaptığımız çalışmaların özetini şu URL'de bulabilirsiniz:

<http://web.engr.oregonstate.edu/~aciicmez/osutass/>

koc@kripito